UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/493,984	01/28/2000	Robert S. Eisenbart	D2317	2907

43471 7590 07/19/2006

GENERAL INSTRUMENT CORPORATION DBA THE CONNECTED
HOME SOLUTIONS BUSINESS OF MOTOROLA, INC.
101 TOURNAMENT DRIVE
HORSHAM, PA 19044

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/493,984	**Applicant(s)** EISENBART ET AL.	
	Examiner Michael J. Simitoski	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-19 and 21-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-19 and 21-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. The response of 5/17/2006 was received and considered.

2. Claims 1, 2, 4-19 & 21-23 are pending.

Response to Arguments

3. Applicant's arguments filed 5/17/2006 have been fully considered but they are not persuasive.

4. Applicant's response (p. 2) argues that the MAC and encrypted control word are transmitted and received together and not separately, regarding the limitation "sending the second information ... separately from ... sending the first information". However, the Examiner is not asserting that Wasilewski's MAC and encrypted control word are sent separately, as clearly seen from §5 of the previous Office Action.

5. Applicant's response (p. 3, ¶1) argues the following:

> "[1] the MSK, which the Examiner equates with the claimed 'first information' is not transmitted or received in the system shown in Figure 3A. The MSK is used in Figure 3A to encrypt the control word and thereby form the encrypted control word. It is the encrypted control word in Figure 3A that is transmitted and received. [2]To further support this conclusion, Applicant notes that the MSK of Wasilewski et al. ('474) is part of a public key/private key encryption. See column 10, lines 31-33. In this type of encryption, one key is used to encrypt the data and a second, different key is used to decrypt the data. There is therefore no need to transmit the first, encrypting key."

Regarding [1] above, the first information/MSK is not transmitted in Fig. 3A because Fig. 3A is only dealing with the ECMs. However, Applicant is directed to Fig. 3B, where the EMM (which contains the MSK) (col. 11, lines 10-15) is transmitted (Fig. 3B & col. 10, lines 31-33). Therefore, contrary to Applicant's assertion, both the ECM (encrypted control words) and the EMM (MSK) are sent. Regarding [2] above, Applicant is directed to col. 10, lines 31-33 where Wasilewski discloses "The public key corresponding to a particular private key is used to encrypt messages (e.g., MSKs) in the CAM prior to transmission to the STUs 90" (emphasis added). Therefore, the MSK is subject to encryption, not part of a public key/private key encryption and as such, Wasilewski does not transmit the encrypting key.

6. Applicant's response (p. 3, ¶2) argues that "the Examiner asserts that the output of SABER 20 in Figure 3A is transmitted in a plurality of packets. However, it is unclear from Wasilewski et al. ('474) if the output of SABER 20 would require more than one packet." Applicant further argues that if the number of bytes being output was small enough they *could* be packaged into one packet. In Wasilewski, the program data is encrypted with the control words (col. 8, lines 10-13), the control words being encrypted using the MSK (col. 8, lines 25-28) and sent to the STU via an ECM (col. 9, lines 16-18). The MSK is encrypted using a public-key algorithm (col. 8, lines 34-37) and sent to the STU via an EMM (col. 11, lines 43-48). Applicant suggests that the ECMs and the EMMs are carried in the same packets. However, Applicant is directed to the following disclosure in Wasilewski:

> "The encrypted control words are sent to the CBI 164 where they are inserted in MPEG-2 transport packets, assigned a unique PID, and transmitted over the backplane to be multiplexed into the stream of transport packets by the control card 22. The MSK is also encrypted and inserted in MPEG-2 transport packets. These transport packets are generated by the CAM 30 but are also routed through the CBI 164 of the conditional access card 24 for output onto the backplane 21. All the transport packets are multiplexed by the control card 22 to form a single outgoing transport stream" (col. 20, line 66 – col. 21, line 9, emphasis added).

Nowhere in Wasilewski are the ECMs and EMMs inserted into the same packet. It is evident from the cited passage that ECMs (encrypted control words) are inserted in transport packets, assigned a unique PID, and transmitted over the backplane to be multiplexed into the stream of transport packets by the control card. The MSK is also encrypted and inserted in transport packets (which are generated by the CAM) and routed through the CBI for output onto the backplane. This notion is further supported by the fact that the CBI inserts the

ECM/encrypted control words into transport packets, but the EMM/MSK is inserted into transport packets that are created by the CAM (not the CBI) and then routed through the CBI to be multiplexed into the transport stream. Further support is provided in U.S. Patent 5,420,866, which is incorporated by reference in Wasilewski et al. ('474) in col. 7, lines 47-51. The '866 patent discloses even more explicitly the packets containing the ECMs and EMMs (Fig. 3B).

7. Applicant's response (p. 3, ¶3) argues that the combination of Wasilewski and Banker, regarding claims 7, 10 & 14, does not arrive at the claimed invention. Applicant asserts that if one having ordinary skill in the art were to combine Wasilewski with Banker, the resulting system would be the transmission of the combination encrypted control word, other data and MAC from SABER 20 over a single out-of-band channel to a set top box in accordance with Banker and the different pieces of data output from SABER 20 would not be transmitted over a plurality of pathways. However, Banker teaches a concept well known in the art such that transmitting data that needs to be received periodically over an out-of-band channel will allow the reception regardless of what channel the receiver/STU is tune to (col. 1, lines 28-44 & col. 2, lines 55-68). This would be particularly applicable to Wasilewski since without the EMM packet (containing the MSK), none of the ECMs could be decrypted and hence no content would be decrypted. Further, the control words are changed often, lending against transmitting them out-of-band (col. 8, lines 48-60); in contrast, the MSKs (EMM) changes at a much lower rate and would therefore be more detrimental if lost, lending towards transmission out-of-band. This losing of important packets is what the Banker reference suggests to improve upon (col. 1, lines 41-44).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-2, 4-6, 8-9, 11-13 & 21 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 5,870,474 to Wasilewski et al. (**Wasilewski**).

Regarding claims 1, 8 & 11, Wasilewski discloses generating a signatory group comprising at least a portion of a first information/MSK and at least a portion of a second information/clear code word (col. 9, lines 31-46), generating a signature over the signatory group (col. 9, lines 31-46), appending the signature/hash to one of the first information or the second information (appended to second information/clear code word) (col. 9, lines 40-46), sending the first information/MSK over a network (col. 11, lines 4-48), sending the second information/clear code word over the network separately from the step of sending the first information (col. 9, lines 40-46) and sending the signature over the network separately from at least one of the first information or the second information (separate from the first information/MSK) (col. 9, lines 31-46, col. 11, lines 4-48 & col. 20, line 66 – col. 21, line 9).

Regarding claims 2 & 9, Wasilewski discloses the first information/MSK comprising an authorization data structure/key (col. 9, lines 47-52) and the second information/clear code word comprising a software object/key (col. 9, lines 30-46).

Regarding claim 4, Wasilewski discloses determining which resources a software object in the second information/clear code word is entitled to interact with (which blocks of packets they can decrypt) (col. 8, lines 48-60).

Regarding claim 5, Wasilewski lacks explicitly waiting a predetermined time period after the step of sending the first information before sending the second information. However, it is inherent that, in a packet-based network, a predetermined time period (transmission rate) is waited between each packet, and hence between each piece of information.

Regarding claim 6, Wasilewski discloses the first information/MSK including authorization information for an associated software object/clear code word (col. 9, lines 30-35).

Regarding claim 12, Wasilewski discloses determining a lifetime for which the second information is usable (col. 8, lines 48-60).

Regarding claim 13, Wasilewski discloses checking the first information/MSK for an authorization corresponding to the second information/clear code word (decrypting) (col. 8, lines 25-28).

Regarding claim 21, Wasilewski discloses determining if access of at least one of the first or second information is authorized (determining if control word is authorized) (col. 9, lines 47-58) and ignoring the second information/control word if not authorized (col. 9, lines 47-58).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 7, 10, 14-15 & 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski**, as applied to claims 1 and 8 above, in view of U.S. Patent 5,247,364 to Banker et al. (**Banker**).

Regarding claims 7 & 10, Wasilewski discloses a system, but lacks sending information over different transmission pathways. Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 14, Wasilewski discloses an information object/MSK, authorization information/clear code word wherein a signature/hash is generated over the information object/MSK and the authorization information/clear code word (col. 9, lines 30-38), wherein the signature/hash is integral to one of the information object or the authorization information (integral with the authorization information/ clear code word) (col. 9, lines 40-46). Wasilewski lacks the information object using a first transmission pathway to a set top box, the authorization information using a second transmission pathway to the set top box that is different from the first transmission pathway and the signature using a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways. However, Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 15, Wasilewski discloses an authorization message/ECM, which includes the authorization information/clear code word and the signature (col. 9, lines 40-46).

Regarding claim 19, Wasilewski discloses the information object/MSK sent separately over a network from the authorization information/clear code word (col. 11, lines 10-15).

12. Claims 16 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski** in view of **Banker**, as applied to claim 14 above, in further in view of U.S. Patent 6,157,721 to Shear et al. (**Shear**). Wasilewski discloses a system, as modified above, that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated

to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

13. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski** in view of **Banker**, as applied to claim 14 above, in further in view of U.S. Patent 5,420,866 to Wasilewski (**Wasilewski '866**). Wasilewski, as modified above, is silent regarding including tiers in the authorization information. However, Wasilewski '866 teaches that satellite and cable access providers include tier information with authorization information sent to decoders to control access to different tiers of programs (col. 4, lines 51-59). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include tier information in the authorization information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of controlling access to different tiers of programs in a television subscription service, as taught by Wasilewski '866 (col. 4, lines 51-59).

14. Claims 22 & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski**, as applied to claims 1 and 8 above, in view of **Shear**. Wasilewski discloses a system that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and

to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS
July 7, 2006

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100